DIALOG(R)File 352:Derwent WPI

013477186 **Image available**
WPI Acc No: 2000-649129/200063
XRPX Acc No: N00-481281
Authentication method using biometrics (fingerprints) for identifying PC user by decrypting message based on calculated secret key
Patent Assignee: NEC CORP (NIDE)
Inventor: UCHIDA K
Number of Countries: 003 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2348309	A	20000927	GB 20007102	A	20000323	200063	B
AU 200022470	A	20000928	AU 200022470	A	20000322	200063	
JP 2000276445	A	20001006	JP 9977697	A	19990323	200065	

Priority Applications (No Type Date): JP 9977697 A 19990323
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2348309	A		62	G06F-001/00	
AU 200022470	A			G06F-012/14	
JP 2000276445	A		10	G06F-015/00	

Abstract (Basic): GB 2348309 A
NOVELTY - A user is identified by entering fingerprint (10) from a portable terminal. When the user has been registered a communication is established between terminal and authentication execution device (2). A common secret code is calculated for transmitting encrypted message (15). The message can only be decrypted based on calculated secret key.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a portable terminal for authentication using biometrics identification, an authentication system using biometrics identification, a computer readable medium storing an authentication program.
USE - For identifying PC user.
ADVANTAGE - It provides security without the trouble of remembering passwords.
DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of the structure of an authentication system using biometrics.
Execution device (2)
Fingerprint Sensor (10)
Encrypted Message (15)
pp; 62 DwgNo 1/7
Title Terms: AUTHENTICITY; METHOD; FINGERPRINT; IDENTIFY; USER; MESSAGE; BASED; CALCULATE; SECRET; KEY
Derwent Class: S05; T01; T04; T05
International Patent Class (Main): G06F-001/00; G06F-012/14; G06F-015/00
International Patent Class (Additional): G06F-015/02; G06K-009/00; G06T-007/00; G07C-009/00; H04L-009/32
File Segment: EPI

06690615 **Image available**

AUTHENTICATION METHOD AND DEVICE USING BIOMETRICS DISCRIMINATION, AUTHENTICATION EXECUTION DEVICE, AND RECORDING MEDIUM RECORDED WITH AUTHENTICATION PROGRAM

PUB. NO.: **2000-276445** [JP 2000276445 A]
PUBLISHED: October 06, 2000 (20001006)
INVENTOR(s): UCHIDA KAORU
APPLICANT(s): NEC CORP
APPL. NO.: 11-077697 [JP 9977697]
FILED: March 23, 1999 (19990323)
INTL CLASS: G06F-015/00; G06F-015/02; G06T-007/00

ABSTRACT

PROBLEM TO BE SOLVED: To obtain an authentication device which has a high security and is free from the trouble that a password is preliminarily stored.

SOLUTION: The fingerprint picture of a user detected by a fingerprint sensor 10 is converted to a digital picture, and its fingerprint features are extracted by a fingerprint feature extraction part 11. Fingerprint feature information and Secret information peculiar to the user are stored in a user information storage part 13. A fingerprint collation part 12 compares stored fingerprint features with fingerprint information stored in the user peculiar information storage part 13 to discriminate whether the user is a registered user or not; and if the user is registered, secret information paired with this fingerprint information is sent to an authentication message encryption part 15. A cipher key consensus part 14 uses random numbers to generate a cipher key, and the authentication message encryption part 15 uses this cipher key to encipher the secret information and sends it from a communication message transmission part 16 to an authentication execution machine 2. This machine 2 uses a cipher key generated by a cipher key consensus part 22 to decipher the message received from a portable terminal 1 by an authentication message deciphering part 23.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－276445
（P2000－276445A）
(43)公開日　平成12年10月６日(2000.10.6)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｆ	５Ｂ０１９
	15/02	３６０	15/02	３６０Ａ	５Ｂ０４３
Ｇ０６Ｔ	7/00		15/62	４６０	５Ｂ０８５

審査請求 有　請求項の数23 ＯＬ （全 10 頁）

(21)出願番号　特願平11－77697

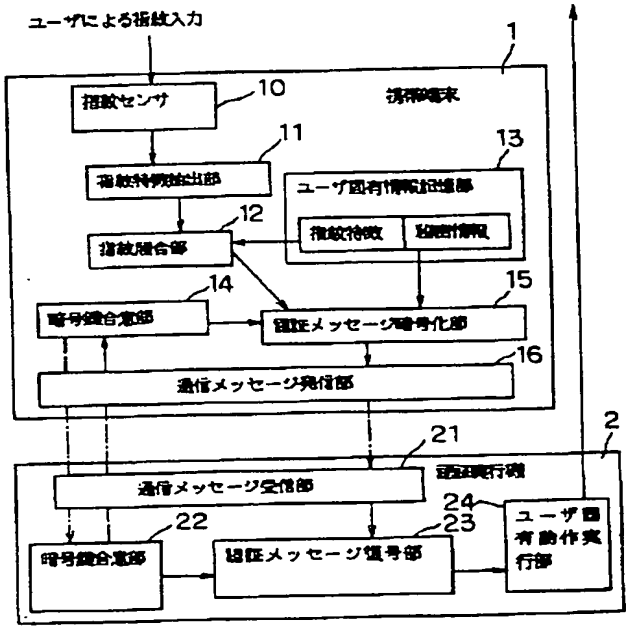
(22)出願日　平成11年３月23日(1999.3.23)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　内田　薫
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100088328
弁理士　金田　暢之　（外２名）

Ｆターム(参考)　5B019 GA02 GA03 JA09
5B043 AA04 AA09 BA02 CA10 FA03 GA01
5B085 AE09 AE23 AE26

(54)【発明の名称】　バイオメトリクス識別を用いた認証方法、装置、認証実行機、認証プログラムを記録した記録媒体

(57)【要約】
【課題】　パスワードを記憶しておく煩雑性がなく、かつセキュリティの高い認証装置を提供する。
【解決手段】　指紋センサ１０で検出されたユーザの指紋画像はデジタル画像に変換され、指紋特徴抽出部１１によってその指紋特徴が抽出される。ユーザ情報記憶部１３は指紋特徴情報と、ユーザに特有な秘密情報を記憶している。指紋照合部１２では指紋特徴をユーザ固有情報記憶部１３に記憶されている指紋情報と比較し、当該ユーザが登録されたユーザであるかどうか判定し、登録されていれば、その指紋情報と対の秘密情報を認証メッセージ暗号化部１５に送る。暗号鍵合意部１４では乱数を用いて暗号鍵を生成し、認証メッセージ暗号化部１５ではこの暗号鍵を用いて秘密情報を暗号化し通信メッセージ発信部１６より認証実行機２に送る。認証実行機２では、携帯端末１から受け取ったメッセージを暗号鍵合意部２２で生成された暗号鍵を用いて、認証メッセージ復号部２３で復号する。



【特許請求の範囲】

【請求項１】　携帯できる認証端末上で、そこに入力されたバイオメトリクスによりユーザを識別し、これが予め登録されたユーザの場合には、認証端末とは独立した認証実行機との間で通信し、認証メッセージ送付に用いる共通の暗号化鍵を合意し、この暗号化鍵に基づいて認証端末上で前記ユーザの固有情報を含む認証メッセージを暗号化し、暗号化した認証メッセージを認証端末から認証実行機に送信し、認証実行機上で認証メッセージを先に合意した暗号化鍵に基づいて復号し、メッセージに含まれたユーザ固有情報に応じた処理を行う、バイオメトリクス識別を用いた認証方法。

【請求項２】　前記通信メッセージが赤外線、無線電波、音波を例とする非接触型通信のうち、いずれかを含む方法により通信される請求項１記載の認証方法。

【請求項３】　前記認証メッセージに含まれるユーザ固有情報が、前記認証端末上でのバイオメトリクスによる正当なユーザであることの識別なしには読み出すことのできない秘密情報を含む請求項１記載の認証方法。

【請求項４】　前記認証実行機側で行うユーザ固有情報に応じた処理が、認証端末上でのバイオメトリクスによる正当なユーザであることの識別なしには実行できない処理であり、したがって予めバイオメトリクスを登録した本人が前記認証端末を持参し使用したことを認証する機能をもつ請求項１記載の認証方法。

【請求項５】　前記認証メッセージに含まれるユーザ固有情報が、認証端末上でのバイオメトリクスによる正当なユーザであることの識別なしには読み出すことのできない個別情報を含み、これを用いて前記認証実行機側ではどのユーザが本認証機能を使用したかの情報を用いた処理を行う請求項１記載の認証方法。

【請求項６】　前記認証実行機側で行うユーザ固有情報に応じた処理が、ファイル内容の暗号化および復号処理を含み、特に本暗号化・復号に用いる暗号鍵が前記認証端末上でのバイオメトリクスによる正当なユーザであることの識別なしには読み出すことのできない方法で保管される請求項１記載の認証方法。

【請求項７】　ユーザのバイオメトリクス画像を取得するバイオメトリクス画像入力手段と、
入力されたバイオメトリクス画像から照合用のバイオメトリクス特徴を抽出するバイオメトリクス特徴抽出手段と、
前記ユーザのバイオメトリクス特徴と固有情報を対で記憶するユーザ固有情報記憶手段と、
認証実行機との認証メッセージの暗号化に用いる鍵を決定するための暗号鍵合意手段と、
今回、ユーザが入力したバイオメトリクス画像から抽出されたバイオメトリクス画像と前記ユーザ固有情報記憶手段に記憶されているバイオメトリクス特徴を比較し、今回バイオメトリクス画像を入力したユーザが登録されたユーザかどうか判定し、登録されたユーザであれば、前記バイオメトリクス画像と対でユーザ固有情報記憶手段に記憶されている固有情報を出力するバイオメトリクス画像照合手段と、
決定された暗号鍵を用いてユーザの前記固有情報を暗号化する認証メッセージ暗号化手段と、
通信メッセージを認証実行機に対して発信する通信メッセージ発信手段とを有する携帯端末。

【請求項８】　前記ユーザ固有情報記憶手段は、複数のユーザについての、バイオメトリクス特徴と固有情報の情報を記憶する、請求項７記載の携帯端末。

【請求項９】　前記バイオメトリクス画像照合手段は、バイオメトリクス画像の類似性に応じたスコアを評価し、該スコアが閾値より高い場合に、今回、バイオメトリクス画像を入力したユーザが登録されたユーザであると判定する、請求項７または８に記載の携帯端末。

【請求項１０】　前記暗号鍵合意手段は、乱数を任意に生成し、前記認証実行機に送付するとともに、該乱数を元として秘密の計算式を用いて前記鍵を計算する、請求項７から９のいずれか１項記載の携帯端末。

【請求項１１】　前記暗号鍵合意手段は、前記鍵を決定するに先立って、予め定めたプロトコルと合い言葉によって前記認証実行機と相互認証する、請求項７から９項のいずれか１項記載の携帯端末。

【請求項１２】　前記暗号鍵合意手段は、乱数を任意に生成し、生成した乱数を前記認証実行機に送付するとともに、前記認証実行機から生成された乱数を受け取り、両乱数を用いて前記鍵を生成する、請求項７から９のいずれか１項記載の携帯端末。

【請求項１３】　赤外線、無線電波、音波を例とする非接触型通信のうち、いずれかを含む通信により前記認証実行機と通信する、請求項７から１２のいずれか１項記載の携帯端末。

【請求項１４】　別の端末を介して前記認証実行機と通信する、請求項７から１３のいずれか１項記載の携帯端末。

【請求項１５】　請求項７から１４のいずれか１項記載の携帯端末との認証メッセージの暗号化に用いる鍵を決定するための暗号鍵合意手段と、
携帯端末から送付された通信メッセージを受信する通信メッセージ受信手段と、　決定された暗号鍵を用いて通信メッセージを復号する認証メッセージ復号手段と、
通信メッセージから復号された固有情報に基づいてユーザ固有の動作を実行するユーザ固有動作実行手段とを有する認証実行機。

【請求項１６】　前記暗号鍵合意手段は、前記携帯端末から送付された乱数を元として、前記携帯端末側と同一の秘密の計算式を用いて前記鍵を計算する請求項１５記載の認証実行機。

【請求項１７】　前記暗号鍵合意手段は、前記携帯端末

から乱数を受け取るとともに、任意の乱数を発生し、両乱数を用いて前記鍵を生成する請求項１５記載の認証実行機。

【請求項１８】　ユーザのバイオメトリクス画像を取得するバイオメトリクス画像入力処理と、
入力されたバイオメトリクス画像から照合用のバイオメトリクス特徴を抽出するバイオメトリクス特徴抽出処理と、
認証実行機との認証メッセージの暗号化に用いる鍵を決定するための暗号鍵合意処理と、
今回、ユーザが入力したバイオメトリクス画像から抽出されたバイオメトリクス画像と、前記ユーザのバイオメトリクス特徴と固有情報を対で記憶するユーザ固有情報記憶手段に記憶されているバイオメトリクス特徴を比較し、今回バイオメトリクス画像を入力したユーザが登録されたユーザかどうか判定し、登録されたユーザであれば、前記バイオメトリクス画像と対でユーザ固有情報記憶手段に記憶されている固有情報を出力するバイオメトリクス画像照合手段と、
決定された暗号鍵を用いてユーザの前記固有情報を暗号化する認証メッセージ暗号化処理と、
通信メッセージを認証実行機に対して発信する通信メッセージ発信処理とを、コンピュータに実行させるための認証プログラムを記録した記録媒体。

【請求項１９】　前記バイオメトリクス画像照合処理は、バイオメトリクス画像の類似性に応じたスコアを評価し、該スコアが閾値より高い場合に、今回、バイオメトリクス画像を入力したユーザが登録されたユーザであると判定する、請求項１８記載の記録媒体。

【請求項２０】　前記暗号鍵合意処理は、乱数を任意に生成し、前記認証実行機に送付するとともに、該乱数を元として秘密の計算式を用いて前記鍵を計算する、請求項１８または１９記載の記録媒体。

【請求項２１】　請求項１８から２０のいずれか１項記載の認証プログラムとの認証メッセージの暗号化に用いる鍵を決定するための暗号鍵合意処理と、
認証プログラムから送付された通信メッセージを受信する通信メッセージ受信処理と、
決定された暗号鍵を用いて通信メッセージを復号する認証メッセージ復号処理と、
通信メッセージから復号された固有情報に基づいてユーザ固有の動作を実行するユーザ固有動作実行処理とをコンピュータに実行させるための認証実行プログラムを記録した記録媒体。

【請求項２２】　前記暗号鍵合意処理は、前記携帯端末から送付された乱数を元として、前記携帯端末側と同一の秘密の計算式を用いて前記鍵を計算する、請求項２１記載の記録媒体。

【請求項２３】　前記暗号鍵合意処理は、前記認証プログラムから乱数を受け取るとともに、任意の乱数を発生し、両乱数を用いて前記鍵を生成する請求項２１または２２記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はバイオメトリクス、すなわち、指紋などの計測可能な生体特徴による照合を利用して利用者本人かどうかを確認し、本人にのみ実行可能な動作を許可する認証方法に関する。

【０００２】

【従来の技術】情報処理装置、例えば、パーソナルコンピュータ（以下ＰＣ）で本人のみが実行できるべき動作として、例えばそのユーザとしてのログイン動作、あるいは電子商取引での本人と確認した上での取引、さらにはファイルの暗号化や復号動作などがある。

【０００３】このような場合、その動作を実行しようとしているのが本人であることを証明するために、従来は、利用者にパスワードを入力させている。この場合、許可を得ようとする者は、予め決められたパスワードを記憶しておかなければならないという煩雑性があり、さらにそのパスワードを盗み見られた場合などは他人でも本人になりすまし、不正な利用をすることができるという問題がある。

【０００４】この問題を解決する方法として、パスワードを使用する代わりに指紋などのバイオメトリクスを使用する方法が提案されている。以下ではバイオメトリクスとして指紋を用いる場合を例に挙げて図５を参照して説明する。

【０００５】本従来法においては、ＰＣに指紋センサ１０を接続し、またＰＣ内のユーザ固有情報記憶部１３にそのユーザの指紋データから抽出した照合用の特徴情報を記憶し、指紋がユーザによって入力された際には指紋特徴抽出部１１において指紋から特徴情報を抽出し、記憶されていた特徴との一致を指紋照合部１２において判断することにより、一致したときにのみ本人と確認し、ユーザ固有動作実行部１７でユーザ固有の動作を実行する。

【０００６】

【発明が解決しようとする課題】このような形態においては、認証を行う装置内で指紋の入力画像および特徴情報が処理されるため、この装置がユーザの管理下にない場合には、このプログラムを不正に改変することにより特徴情報が盗まれる危険性がある。これを防ぐためにはユーザの管理下にあり、ユーザが持参する携帯型の端末、例えば、電子手帳のような情報端末であるとかあるいはＩＣカードなどの媒体上に、図５のユーザ固有情報記憶部１３に相当する指紋の特徴情報を保持して、その内容をＰＣ側に転送して照合を行うという方法もある。しかしこれでも指紋センサが管理の十分でないＰＣに接続されていると、指紋入力を制御するプログラムを不正に改変することにより、その指紋センサで指紋が入力さ

れた際に複写保存しておいた他人の指紋画像やあるいは他で入手した指紋画像を、あたかも指紋センサで自分が入力した如く装うことによりなりすましを実現できるという可能性がある。

【０００７】一方、上記のような携帯型の端末は持ち運びができてそれを持参すれば任意の場所で本人確認ができるという利点があるが、この端末をＰＣに挿入し、あるいはこれとＰＣとをいちいちケーブルで結線して接続してから認証動作を行うのは煩雑である。そこで、赤外線・無線電波・音波などの非接触型の方法を用いて通信させることでこれら両者の間のデータ交換を行うという方法がある。しかしこれらの信号は容易に盗聴可能であり、データ信号を第三者が受信してこれを再利用することで正当なユーザになりすます、という問題点が生じる。

【０００８】本発明の目的は、パスワードを記憶しておく煩雑性がなく、さらに他人によるなりすましが不可能で、かつ携帯に適するように赤外線・無線電波・音波などで端末とＰＣとを通信させ、かつ指紋データが盗まれあるいはメッセージを不正に再利用される可能性のないセキュリティの高い認証方法および装置を提供することである。

【０００９】

【課題を解決するための手段】本発明は、携帯できる認証端末上で、そこに入力されたバイオメトリクスによりユーザを識別し、これが予め登録されたユーザの場合には、認証端末とは独立した認証実行機との間で通信し、認証メッセージ送付に用いる共通の暗号化鍵を合意し、この暗号化鍵に基づいて認証端末上で前記ユーザの固有情報を含む認証メッセージを暗号化し、暗号化した認証メッセージを認証端末から認証実行機に送り、認証実行機上で認証メッセージを先に合意した暗号化鍵に基づいて復号し、メッセージに含まれたユーザ固有情報に応じた処理を行うことを特徴とする。

【００１０】ここで、携帯端末は、ユーザのバイオメトリクス画像を取得するバイオメトリクス画像入力手段と、入力されたバイオメトリクス画像から照合用のバイオメトリクス特徴を抽出するバイオメトリクス特徴抽出手段と、前記ユーザのバイオメトリクス特徴と固有情報を対で記憶するユーザ固有情報記憶手段と、認証実行機との認証メッセージの暗号化に用いる鍵を決定するための暗号鍵合意手段と、今回、ユーザが入力したバイオメトリクス画像から抽出されたバイオメトリクス画像とユーザ固有情報記憶手段に記憶されているバイオメトリクス特徴を比較し、今回バイオメトリクス画像を入力したユーザが登録されたユーザかどうか判定し、登録されたユーザであれば、前記バイオメトリクス画像と対でユーザ固有情報記憶手段に記憶されている固有情報を出力するバイオメトリクス画像照合手段と、決定された暗号鍵を用いてユーザの前記固有情報を暗号化する認証メッセージ暗号化手段と、通信メッセージを認証実行機に対して発信する通信メッセージ発信手段とを有する。

【００１１】また、認証実行機は、携帯端末との認証メッセージの暗号化に用いる鍵を決定するための暗号鍵合意手段と、携帯端末から送付された通信メッセージを受信する通信メッセージ受信手段と、決定された暗号鍵を用いて通信メッセージを復号する認証メッセージ復号手段と、通信メッセージから復号された固有情報に基づいてユーザ固有の動作を実行するユーザ固有動作実行手段とを有する。

【００１２】本発明は、入力するバイオメトリクスによりユーザの識別を行い、これが登録したものと一致したときにのみ登録されたユーザ固有動作を実行する。特にバイオメトリクスの入力と特徴抽出、および照合処理をユーザが携帯する端末上で行い、さらにユーザ固有動作を実行する認証実行機との間の通信は携帯端末と認証実行機の間で合意したその通信固有の暗号鍵で暗号化することにより、装置全体の高いセキュリティを実現している。

【００１３】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００１４】図１を参照すると、本発明の一実施形態の認証装置は携帯端末１と認証実行機２から構成される。

【００１５】携帯端末１は、指紋センサ１０、指紋特徴抽出部１１、指紋照合部１２、ユーザ固有情報記憶部１３、暗号鍵合意部１４、認証メッセージ暗号化部１５、通信メッセージ発信部１６で構成される。認証実行機２は、通信メッセージ受信部２１、暗号鍵合意部２２、認証メッセージ復号部２３、ユーザ固有動作実行部２４で構成される。

【００１６】指紋センサ１０はユーザの指が接触した際にその指紋画像を撮影し、その画像データを指紋特徴抽出部１１で処理可能なようにデジタル画像データに変換する。指紋センサ１０の構成法としては例えばＬＥＤで発せられた光をプリズムで反射し、このとき反射面の外側に置かれた指の隆線に従い、隆起部と谷部で反射率が異なることを利用し、ＣＣＤを用いて反射光をデジタル映像化することで指紋画像を撮影する光学方式ものを用いることができる。あるいは、IEEEE ISSCC98. SA 17. 7. pp. 285-285(1998. 2) の「A Robust, 1. 8V, 250uW, Direct Contact500dpi Fingerprint Sensor」(Inglis et al.)に記載されたような、静電容量検知方式による指紋センサを利用すればさらに携帯に適した小型薄型の指紋センサが実現できる。この静電容量検知方式においては、センサに皮膚が接する指紋の隆線隆起部と空気層が間に存在する谷部との、センサが検知する静電容量の差を計測することにより、指紋の隆線形状をデジタル画像化することで指紋画像を撮影する。

【００１７】指紋特徴抽出部１１では、指紋センサ１０

より得られた指紋画像を受取り、ここから指紋の識別に用いる特徴を抽出する処理を実行する。特徴抽出の実現法としては、例えば次の文献に記述された方法がある。浅井　紘、星野幸夫、木地和夫、「マニューシャネットワーク特徴による自動指紋照合‥特徴抽出課程‥」電子情報通信学会論文誌、vol. J72-D-II. No. 5、ページ７４２～７３２（１９８９年５月）。ここでは隆線を含む濃淡画像から二値化処理・細線化処理による隆線パターンを抽出し、その端点と分岐点の位置を検出した後に、それら相互間を結ぶ線分上の交差隆線数を計数し、その関係図をデジタルデータ表現することにより照合のための指紋特徴としている。

【００１８】ユーザ固有情報記憶部１３は上記のような形式の指紋特徴情報とその指紋の持ち主であるユーザに特有なユーザ固有情報（秘密情報）を対にして記憶しておく部分である。ここでいうユーザ固有情報とは、コンピュータが扱うデータのうち、ユーザ個人に関し有用な情報のあらゆる形態を含むデータのことであり、ユーザを識別するユニークな識別子、あるいはそのユーザだけが閲覧アクセスを許されるデータ、例えばコンピュータへのログインに用いるパスワードであるとか、電子商取引において本人であることを証明する秘密の文字数字列（暗証番号あるいはパスワード）などを含む。新たなユーザ固有情報対を記憶させる際は、記憶させるべきユーザ固有情報を携帯端末のペン入力部などから入力するとともにそのユーザの指紋を指紋センサ１０から入力し、それを元に指紋特徴抽出部１１で得られた指紋特徴との対をユーザ固有情報記憶部１３に記憶させればよい。ユーザ固有情報記憶部１３にはその認証装置のユーザ１人の指紋とその秘密情報だけを保持しておいてもよいし、複数のユーザについてそれらの指紋と秘密情報の対を保持しておいてもよい。

【００１９】指紋照合部１２は、今回ユーザが入力した指紋から得られた指紋特徴Ｓを特徴抽出部１１から、一方これまでに記憶させられている指紋特徴情報Ｆおよびそれと対になってユーザ固有情報記憶部１３に記憶されている秘密情報をユーザ固有情報記憶部１３から入力し、指紋特徴情報Ｆとユーザが入力した指紋から得られた指紋特徴Ｓを比較し、それらの情報が同一の指から得られたものであるときに高くなるような、類似性に応じたスコアを評価する機能を含む。このスコアを予め設定された閾値と比較することで、その指紋情報Ｓを与えたユーザが登録されたユーザと同一であるか否かを判定し、これが閾値より高い場合に「指紋は一致」という識別結果によって、その指紋と対の秘密情報を認証メッセージ暗号化部１５へ出力する。このような指紋を使った押捺者識別のための照合の実現法としては、例えば次の文献に記述された方法がある。浅井　紘、星野幸夫、木地和夫、「マニューシャネットワーク特徴による自動指紋照合‥照合課程‥」電子情報通信学会論文誌、vol. J72-D-II. No. 5、ページ７３３～７４０（１９８９年５月）。ここでは隆線の端点と分岐点相互間を結ぶ線分上の交差隆起線数を計数してデジタルデータ表現したもの同士で位置合わせを行い、その後にそれらの間の類似性を評価することにより照合を実現している。

【００２０】本実施形態で用いている指紋特徴は、押捺指紋間の位置ずれや歪みがあっても安定して正しい照合結果を得られ、同一の指では上記スコアが十分高い一方、異なる指紋ではスコアがほとんどゼロに近くなるという特徴を持ち、また入力となった指紋画像に比べデータサイズがはるかに小さく、照合の演算処理量が小さくてすむ、という利点がある。

【００２１】指紋照合の結果、入力された指紋がユーザ固有情報記憶部１３に記憶された指紋特徴と一致した場合、ユーザ固有情報記憶部１３に記憶されている、そのユーザに関する秘密情報を認証実行機２に送ることになる。この動作は次のように行う。まず暗号鍵合意部１４が今回の通信用の暗号鍵の元となる乱数Ｒを任意に生成し、認証実行機２側の暗号鍵合意部２３に対してこれを送付する。送付には例えば双方に用意された赤外線通信ポート同士の赤外線通信を利用する。暗号鍵合意部１４では送付した乱数Ｒを元として、秘密の計算式を用いてメッセージ暗号化の秘密鍵Ｋを計算する。この計算法としては例えばハッシュ関数を利用することができる。一方、認証実行機２側の暗号鍵合意部２２でも、送付された乱数Ｒを元として、同一の秘密の計算式を用いてメッセージ暗号化の秘密鍵Ｋを計算する。すなわちこの計算式は本認証装置の携帯端末１と認証実行機２の対に固有、かつ秘密の式であり、乱数Ｒを盗聴したとしても、これら以外の装置では秘密鍵Ｋを計算することはできない。

【００２２】認証メッセージ暗号化部１５は、暗号鍵合意部１４が計算した秘密鍵Ｋを用いて、ユーザ固有情報記憶部１３から受け取った指紋照合で一致したユーザの秘密情報を暗号化し、通信によるメッセージを生成する。この暗号化には、例えば、ＤＥＳなどの秘密共通鍵暗号方式を利用する。

【００２３】通信メッセージ発信部１６は認証メッセージ暗号化部１５から受け取った暗号化されたメッセージを認証実行機２に対して送付する。送付には例えば双方に用意された赤外線通信ポート同士の赤外線通信を利用する。

【００２４】認証実行機２では携帯端末１からの通信メッセージを通信メッセージ受信部２１で受け取り、それを認証メッセージ復号部２３に送る。認証メッセージ復号部２３では暗号鍵合意部２２から予め秘密に計算された暗号鍵Ｋを受け取り、それを秘密共通鍵として用いてその暗号を復号する。

【００２５】これにより、携帯端末１の中に保存され、ユーザ本人の正しい指紋の入力によってのみ参照可能な

秘密情報が、盗聴されることなく認証実行機２に送られることになる。認証実行機２ではこれを用いてユーザ固有動作実行部２４において、その秘密情報を用いた動作を実行する。これは例えばコンピュータへの本人としてのログインを許可するであるとか、本人の秘密ファイルの内容を読み出し可能な形で認証実行機２のディスプレイ上に表示することであるとか、あるいは認証実行機２が他の情報処理装置に対して携帯端末１を持参し、指紋を入力したユーザが正当なユーザであることを保証する。さらには電子商取引において本人であることを証明する文字数字列を認証実行機２を経由してネットワークで結ばれた電子商取引提供社側へ送信するなどである。

【００２６】以上のような動作により、携帯端末１上で指紋を入力したユーザが予め登録されたユーザである場合に限り、携帯端末１内に保持される、正しいバイオメトリクスの入力なしには読み出すことのできない秘密情報が安全に認証実行機２に送信され、認証実行機２はユーザの認証を行うことができることになる。また、暗号鍵合意部２２においてこの秘密情報の通信に特有な暗号鍵を発信側である携帯端末１と発信側である認証実行機２の両者で合意しそれを用いるために、赤外線などを用いた過去の通信を傍受し、記録して再生したとしても秘密情報の中身を復号したり、他人になりすまして秘密情報を送ったりすることはできない。

【００２７】なお、上記の説明では暗号鍵合意部１４が乱数を発生し暗号鍵合意部２２に対して一方的にこれを送るという最も簡易な方法を記述したが、さらに安全性を高めるには予め携帯端末１と認証実行機２が通信の相手方が正当な相手であるかどうかを予め定められたプロトコルと合い言葉によって相互認証するという方法もある。さらに、乱数についても、携帯端末１側が一方的に生成するだけでなく、携帯端末１側が生成した乱数Ｒ１と認証実行機２が生成した乱数Ｒ２を互いに交換し、暗号共通鍵の生成にはこれらをつなぎ合わせたものであるとか加算したものであるとかのように両者が揃ったときに初めて動作するような方法で合意することも可能であり、その方が安全性がより高まると考えられる。

【００２８】次に、本実施形態の具体例を説明する。具体例としては、パーソナルコンピュータ（ＰＣ）へのログイン認証を行う場合を考える。各ユーザは自分の携帯端末１を持ち歩き、そこのユーザ固有情報記憶部１３には自分の適当な指の指紋の特徴データと、通常の方法で読み出せない秘密データとしてログインに用いるユーザ名とパスワードが記憶されているとする。この場合、ＰＣが認証実行機２となり、また携帯端末１と認証実行機２との間は赤外線を用いてデータ通信を行うとする。

【００２９】ユーザがＰＣへログインを行おうとする場合、ユーザは携帯端末１の指紋センサ１０に対して、登録してある指紋を入力する。指紋画像がセンサ１０で入力され、指紋特徴抽出部１１でその照合用の特徴が抽出され、指紋照合部１２において、ユーザ固有情報記憶部１３の指紋特徴と照合される。これらが一致した場合には、前記で説明したような方法によって暗号鍵が合意され、それを用いて暗号化されたユーザ名とログインパスワードが携帯端末１からＰＣへ送られる。ＰＣでは認証メッセージ復号部２３においてそのデータを復号した後に、ユーザ固有動作の一例として、ユーザ名とログインパスワードを使用し、ログイン動作を実行する。

【００３０】このような動作によって、携帯端末１上に正当なユーザの正しい指紋が入力されたときにのみ、ログインが許可されることになる。この場合、ユーザはパスワードを覚えておくという煩雑性もまた忘れてログインできなくなるという恐れもなく、一方正しい指紋を入力しなければパスワードという秘密情報は読み出されずログイン動作は実行されないので、なりすましを防ぐこともできる。また、その端末を携帯できるという利便性があり、しかも端末１とＰＣとは赤外線で通信するのでケーブルで結線したり端末１をＰＣに挿入したりという煩雑な動作を実行しないですむ一方、赤外線通信を盗聴されてもメッセージは暗号化されているのでパスワード解読されず、また通信内容を記録され他者によって再生されても暗号鍵が毎回異なっているので他者が不正になりすますことができないとようなログイン認証を実現することができる。

【００３１】なお、この説明では単なるＰＣへのログイン動作として説明したが、このＰＣがネットワークを介して例えば電子商取引を行うシステムのユーザ用端末として使用されている場合には、その取引における本人確認にも使える。その場合、携帯端末１上に記憶される秘密情報がユーザの顧客識別番号と、暗証番号などの本人確認用の情報であると考えればよい。その場合、この秘密情報が携帯端末１から電子商取引を行うシステムのユーザ用端末に送られ、さらにユーザ用端末は携帯端末１から送信された本人確認用の情報を、必要に応じ独自に暗号化を施した後に電子商取引の認証ホストへ送信し、認証ホストがそこに記憶された情報との一致を調べることで本人の確認を行う。

【００３２】さらに、この場合、ユーザが持参する携帯端末１はいわゆる情報端末でなく、カード状のものであった方がより携帯のための利便性が優れている。一般にＩＣカードと呼ばれるような集積回路を搭載できるカード上に指紋センサと計算およびデータ記憶用のチップを搭載することで、このような電子商取引のユーザ用端末と赤外線で通信する携帯用の認証カードを実現できる。

【００３３】なお、上記の説明では携帯端末１と認証実行機２の間は赤外線で通信すると説明したが、これは無線や超音波に代えることも可能であるし、もちろん携帯端末１と認証実行機２とをケーブルで結線したり、あるいは携帯端末１を認証実行機２に挿入したり、密着させたりして何らかの電気的・磁気的手段で通信させても基

本的動作は同様である。

【００３４】なお、上記の説明では各ユーザが自分専用の携帯端末を携帯し、携帯端末には一人のユーザのデータしか記録しないと述べているが、携帯端末に複数の指とそれぞれの秘密情報を記憶しておいて、登録しているユーザの誰でもそこに指紋を入力すれば、その本人の秘密情報のみが認証実行機に送られるような認証装置を実現することももちろん可能である。この場合、指紋照合部１２は、Ｎ対分記憶させてある各指紋特徴情報Ｆとユーザが入力した指紋から得られた指紋特徴Ｓを比較するという動作をＮ回繰り返し、最も高いスコアを持つ指紋特徴情報Ｆを発見することで、その指紋情報Ｓを与えたユーザを特定することになる。さらに上述の実現法のように異なる指紋間ではスコアがほとんど０であるのに対し同一指紋間では誤りなく高いスコアを出すという照合アルゴリズムの場合、Ｎ回繰り返すことなく、ある閾値以上の高いスコアがでた時点で停止し、そのスコアを与えた指紋情報Ｆをもって一致した指紋情報であると判定することもできる。さらに、Ｎ回繰り返してもすべては閾値より低いスコアであった場合には、ユーザの特定を行わずに「特定不能」というメッセージを発するようにすることができる。

【００３５】上記の例では、認証実行機２が携帯端末１と赤外線などで直接通信可能な場合について述べた。さらに、この２者の間に通信の仲介をする端末を置き、遠隔のマシン間で認証を実現することもできる。この第２の実施形態について、図２を参照して説明する。これは第１の実施形態の変形であるが、電子商取引などにおいて、取引サービスの提供者が認証実行機２を運営し、店舗などがその設置端末を管理し、そこにユーザが例えばＩＣカード形状の、商取引会員に身分を証明するための携帯端末１を持参するとする。ここで、ユーザは前記の説明と同じように指紋入力により自分が正当な利用者であること証明する。携帯端末１は設置端末のメッセージ転送部３の仲介を受けて認証実行機２との間で暗号鍵を合意し、これを用いて自己の正当性を証明する秘密情報を認証実行機２に対して送付し、所望の認証を実現することができる。

【００３６】この場合、携帯端末１と設置端末の間は、両者の直接接続やケーブルによる結線、あるいは赤外線のような非接触型の通信で結ばれ、設置端末と認証実行機２の間は電話線や専用ネットワークなどによって通信し、設置端末は単に通信方法の仲介としてメッセージの内部を見ずにその翻訳を行うことになる。

【００３７】このように、携帯端末１と認証実行機２の間に仲介手段があっても直接に暗号鍵を合意し、暗号メッセージを交換することで、途中の設置端末が悪意ある監理者によって運営されていても秘密情報のセキュリティが保たれるシステムを実現できる。

【００３８】図１を参照して本発明の第３の実施形態を説明する。本実施形態としては、パーソナルコンピュータ（ＰＣ）上で、そこに保存されたファイルが他人に読み出されないように、ファイル内容の暗号化を行う場合を考える。各ユーザは自分の携帯端末１を持ち歩き、そこのユーザ固有情報記憶部１３には自分の適当な指の指紋の特徴データと、通常の方法では読み出せない秘密データとしてファイル暗号化に用いる暗号化鍵が記憶されているとする。この場合、ＰＣが認証実行機２となり、また携帯端末１と認証実行機２との間は赤外線を用いてデータ通信を行うとする。ユーザがＰＣのファイルの暗号化を行おうとする場合、ユーザはファイルを指定した後に、携帯端末１の指紋センサ１０に対して登録してある指紋を入力する。指紋画像がセンサ１０で入力されると、前記実施形態で説明したような方法によって指紋の照合が実行され、通信用の暗号鍵が合意され、それを用いて暗号化されたファイル暗号用の暗号鍵Ｋ２が携帯端末１からＰＣへ送られる。ＰＣでは認証メッセージ復号部２３においてそのデータを復号した後に、ユーザ固有動作の一例として、暗号鍵Ｋ２を使用し、指定されたファイルの暗号化動作を実行する。暗号にはＤＥＳなどの共通鍵暗号方式を用いることとする。暗号化されたファイルは中身を読むことができない。

【００３９】ユーザがＰＣ上にあるこのファイルの復号（暗号の解除による内容の復帰）を行おうとする場合、ユーザは暗号化済みファイルを指定した後に、携帯端末１の指紋センサ１０に対して登録してある指紋を入力する。指紋画像がセンサ１０で入力されると、前記実施形態で説明したような方法によって指紋の照合が実行され、通信用の暗号鍵が合意され、それを用いて暗号化されたファイル暗号用の暗号鍵Ｋ２が携帯端末１からＰＣへ送られる。ＰＣでは認証メッセージ復号部２２においてそのデータを復号した後に、ユーザ固有動作の一例として、暗号鍵Ｋ２を使用し、指定され暗号化済みのファイルの復号動作を実行する。これによりファイルの内容は復帰され、読める形になる。

【００４０】このような動作によって、特定の携帯端末上に正当なユーザの正しい指紋が入力されたときにのみ、復号動作が許可され、ファイルの復号が実行されることになる。この場合、そのユーザの携帯端末に対して正しい指紋を入力しなければファイルの復号は実行されないので、ファイル内容の秘匿を実現することができる。また、その端末は小型で携帯できるという利便性がある。

【００４１】なお、本発明ではバイオメトリクスの一例として指紋に限って説明しているが、指紋センサと指紋特徴抽出部の部分を別のバイオメトリクス（個人に固有の生体特徴）を入力し、照合用の特徴を抽出する手段で置換すれば、掌紋・顔・虹彩・網膜血管パターン・掌形、筆跡・声紋など他のバイオメトリクスを使用することも可能である。

【００４２】図３は携帯端末１をソフトウエアを用いて実施する場合のブロック図である。携帯端末は入力装置４１と記憶装置４２，４３と通信装置４４と記録媒体４５とデータ処理装置４６で構成されている。入力装置４１は指紋センサ１０に相当する。記憶装置４２はユーザ固有情報記憶部１３に相当する。記憶装置４３はハードディスクである、通信装置４４は通信メッセージ発信部４４に相当する。記憶媒体４５はＦＤ（フロッピィ・デッィスク）、ＣＤ－ＲＯＭ、ＭＯ（光磁気ディスク）などの記録媒体で、図１および図２携帯端末１の構成のうち、指紋センサ１０の通信メッセージ発信部１６のハードウェア部分を除いた各部から構成される認証プログラムを記録している。データ処理装置４６は記録媒体４５から認証プログラムを記憶装置４３に読み込んだ後、これを実行するＣＰＵである。

【００４３】図４は認証実行機２をソフトウェアを用いて実施する場合のブロック図である。認証実行機は通信装置５１と記憶装置５２と出力装置５３と記録媒体５４とデータ処理装置５５で構成されている。通信装置５１は図１および図２中の通信メッセージ受信部２１に相当する。記憶装置５２はハードディスクである、出力装置５３はユーザ固有動作実行部２４の実行結果が出力される出力装置である。記録媒体５４は記録媒体４５と同様の記録媒体で、図１および図２に示す認証実行機２の構成のうち、通信メッセージ受信部２１のハードウェア部分を除いた各部から構成される認証実行プログラムが記録されている。データ処理装置５５は記録媒体５４から認証実行プログラムを記憶装置５２に読み込んだ後、これを実行するＣＰＵである。

【００４４】

【発明の効果】以上説明したように、本発明は下記のような効果がある。

【００４５】１）バイオメトリクスによる識別技術を利用することで、パスワードを記憶しておく煩雑性がなく、さらに他人によるなりすましが不可能な本人認証装置を実現できる。

【００４６】２）さらに、バイオメトリクスデータをユーザの管理下にある携帯端末内に保持し、かつバイオメトリクスの入力から特徴抽出、照合までを携帯端末内で実行することで、バイオメトリクス情報の管理を容易にし、不正な流出を防ぐことができる。また、この携帯端末は小型化・軽量化により携帯に便利という利便性を生かすことができる。

【００４７】３）また、赤外線・無線電波・音波などで該携帯端末と認証実行機とを通信させることで、ケーブルで結線したり端末をＰＣに挿入したりという煩雑な動作を実行しないで済む。

【００４８】４）赤外線通信などを盗聴されてもメッセージは暗号化されているのでパスワードは解読されない。

【００４９】５）通信内容を記録され他者によって再生されても暗号鍵が毎回異なっているので他者が不正にそれを利用することができない。

【図面の簡単な説明】

【図１】本発明の一実施形態の認証装置の構成図である。

【図２】本発明の他の実施形態の認証装置の構成図である。

【図３】携帯端末をソフトウェアを用いて実施する場合の構成図である。

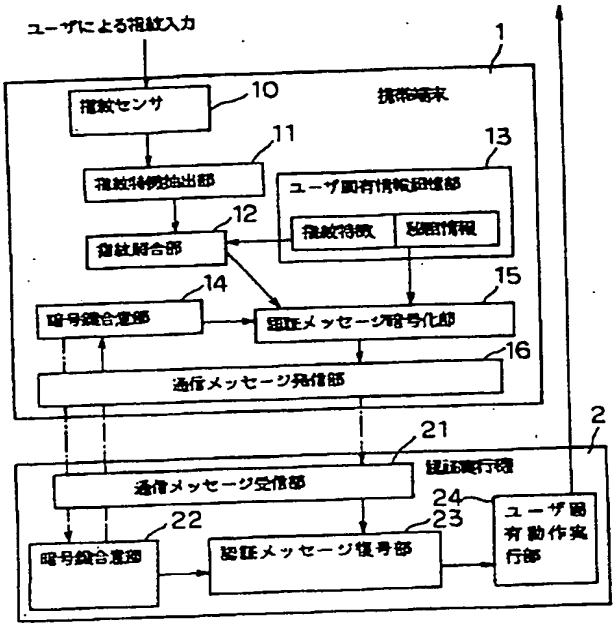
【図４】認証実行機をソフトウェアを用いて実施する場合の構成図である。

【図５】認証装置の従来例の構成図である。

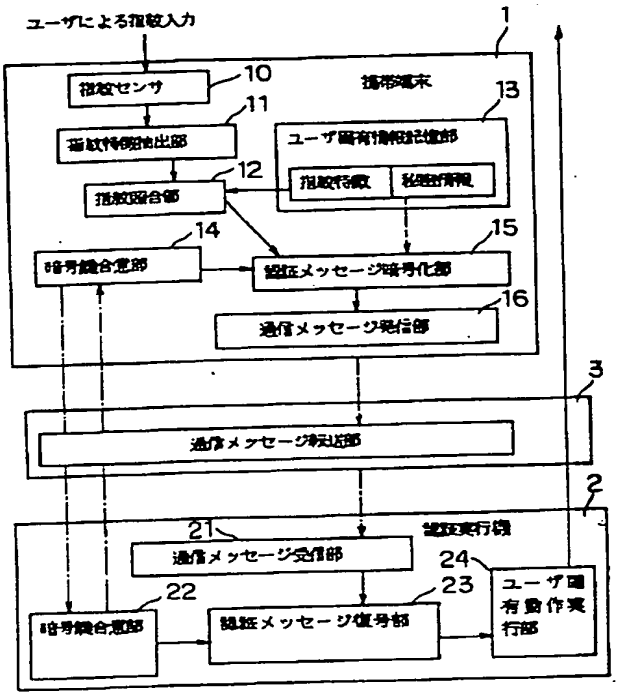
【符号の説明】

１　携帯端末
２　認証実行機
３　通信メッセージ転送部
１０　指紋センサ
１１　指紋特徴抽出部
１２　指紋照合部
１３　ユーザ固有情報記憶部
１４　暗号鍵合意部
１５　認証メッセージ暗号化部
１６　通信メッセージ発信部
２１　通信メッセージ受信部
２２　暗号鍵合意部
２３　認証メッセージ復号部
２４　ユーザ固有動作実行部
４１　入力装置
４２，４３　記憶装置
４４　通信装置
４５　記録媒体
４６　データ処理装置
５１　通信装置
５２　記憶装置
５３　出力装置
５４　記録媒体
５５　データ処理装置

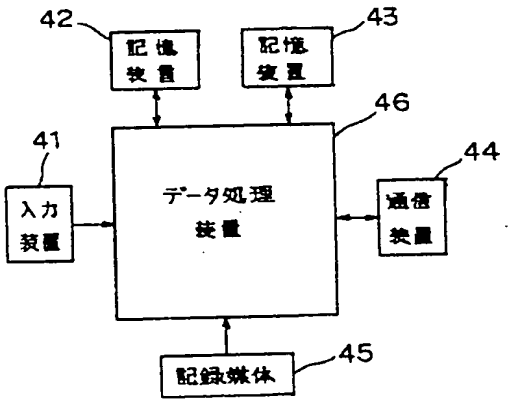
【図１】


ユーザによる指紋入力
1
指紋センサ
10
携帯端末
指紋特徴抽出部
11
ユーザ固有情報記憶部
13
指紋特徴
秘匿情報
指紋照合部
12
暗号鍵合意部
14
認証メッセージ暗号化部
15
通信メッセージ発信部
16
2
認証実行機
通信メッセージ受信部
21
暗号鍵合意部
22
認証メッセージ復号部
23
ユーザ固有動作実行部
24

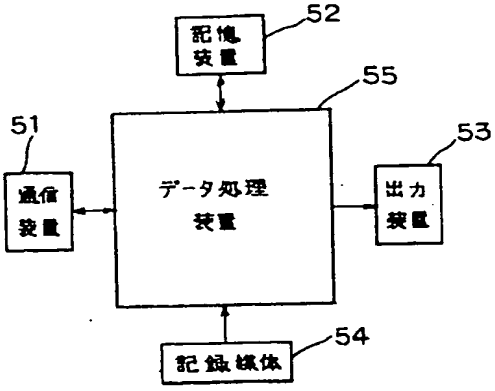
【図２】


ユーザによる指紋入力
1
指紋センサ
10
携帯端末
指紋特徴抽出部
11
ユーザ固有情報記憶部
13
指紋特徴
秘匿情報
指紋照合部
12
暗号鍵合意部
14
認証メッセージ暗号化部
15
通信メッセージ発信部
16
3
通信メッセージ転送部
2
認証実行機
通信メッセージ受信部
21
暗号鍵合意部
22
認証メッセージ復号部
23
ユーザ固有動作実行部
24

【図３】


42
記憶装置
43
記憶装置
46
41
入力装置
データ処理装置
44
通信装置
記録媒体
45

【図４】


記憶装置
52
55
51
通信装置
データ処理装置
出力装置
53
記録媒体
54